IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re U.S. Patent Application of)
)
YAMAMOTO et al.)
)
Application Number: 09/918,642)
)
Filed: August 1, 2001)
)
For: METHOD FOR OBTAINING A SOLUTION OF AN OPTIMIZATION PROBLEM)

Honorable Assistant Commissioner
for Patents
Washington, D.C. 20231

NOTICE OF PRIORITY
UNDER 35 U.S.C. § 119
AND THE INTERNATIONAL CONVENTION

Sir:

In the matter of the above-captioned application for a United States patent, notice is hereby given that the Applicant claims the priority date of April 24 2001, the filing date of the corresponding Japanese patent application 2001-125279.

The certified copy of corresponding Japanese patent application 2001-125279 is being submitted herewith. Acknowledgment of receipt of the certified copy is respectfully requested in due course.

Respectfully submitted,

Stanley P. Fisher
Registration Number 24,344

JUAN CARLOS A. MARQUEZ
Registration No. 34,072

REED SMITH HAZEL & THOMAS LLP
3110 Fairview Park Drive
Suite 1400
Falls Church, Virginia 22042
(703) 641-4200
September 12, 2001

2123

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re U.S. Patent Application of)
)
YAMAMOTO et al.)
)
Application Number: 09/918,642)
)
Filed: August 1, 2001)
)
For: METHOD FOR OBTAINING A SOLUTION OF AN OPTIMIZATION PROBLEM)

Honorable Assistant Commissioner
for Patents
Washington, D.C. 20231

LETTER

Sir:

The below-identified communications are submitted in the above-captioned application or proceeding:

(X)	Priority Document (1)	( ) Verified English Translation
(X)	Notice of Priority	( ) Information Disclosure Statement
( )	Response to Missing Parts with executed declaration	( ) Notice of Related Applications
		( ) Check for $.00

☒ The Commissioner is hereby authorized to charge payment of any fees associated with this communication, including fees under 37 C.F.R. § 1.16 and 1.17 or credit any overpayment to **Deposit Account Number 08-1480**. A duplicate copy of this sheet is attached.

Stanley P. Fisher
Registration Number 24,344

JUAN CARLOS A. MARQUEZ
Registration No. 34,072

REED SMITH HAZEL & THOMAS LLP
3110 Fairview Park Drive
Suite 1400
Falls Church, Virginia 22042
(703) 641-4200

September 12, 2001

日　本　国　特　許　庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００１年　４月２４日

出願番号
Application Number: 特願２００１－１２５２７９

出願人
Applicant(s): 株式会社日立製作所

２００１年　７月２７日

特許庁長官
Commissioner,
Japan Patent Office　及川耕造

出証番号　出証特２００１－３０６５３７４

【書類名】　特許願

【整理番号】　H100217I

【提出日】　平成13年 4月24日

【あて先】　特許庁長官　殿

【国際特許分類】　G06F 17/00

G09C 5/00

【発明者】

【住所又は居所】　東京都国分寺市東恋ケ窪一丁目２８０番地　株式会社日立製作所　中央研究所内

【氏名】　山本　有作

【発明者】

【住所又は居所】　東京都国分寺市東恋ケ窪一丁目２８０番地　株式会社日立製作所　中央研究所内

【氏名】　直野　健

【発明者】

【住所又は居所】　東京都国分寺市東恋ケ窪一丁目２８０番地　株式会社日立製作所　中央研究所内

【氏名】　伊藤　智

【特許出願人】

【識別番号】　000005108

【氏名又は名称】　株式会社日立製作所

【代理人】

【識別番号】　100099298

【弁理士】

【氏名又は名称】　伊藤　修

【連絡先】　０３－３２５１－３８２４

【選任した代理人】

【識別番号】　100099302

【弁理士】

【氏名又は名称】　笹岡　　茂

【手数料の表示】

【予納台帳番号】　018647

【納付金額】　　21,000円

【提出物件の目録】

【物件名】　　明細書　1

【物件名】　　図面　1

【物件名】　　要約書　1

【プルーフの要否】　　要

【書類名】　明細書

【発明の名称】　問題の解取得方法および最適化問題の解取得方法

【特許請求の範囲】

【請求項１】　入力された問題に対する解を要求する解要求装置から求解装置に問題を送り、該求解装置で問題の解を求め前記解要求装置に送り、該解要求装置で解を出力する問題の解取得方法であって、

前記解要求装置は、入力された問題を暗号鍵により暗号化し、該暗号化した問題を前記求解装置に送り、

該求解装置は、送られた暗号化した問題を暗号化したままの状態で解いて解を求め、該求めた解を前記解要求装置に送り、

該解要求装置は、送られた解を前記暗号鍵により復号化し、復号化した解を出力することを特徴とする問題の解取得方法。

【請求項２】　入力された最適化問題に対する解を要求する解要求装置から求解装置に問題を送り、該求解装置で最適化問題の解を求め前記解要求装置に送り、該解要求装置で解を出力する最適化問題の解取得方法であって、

前記解要求装置は、適当に定めた変数変換$y=u(x)$および式の同値変形によって、該最適化問題を異なる等号制約条件$g'(y)=0$，不等号制約条件$h'(y)\geqq 0$，目的関数$f'(y)$を持つ別の最適化問題に変換し、該変換した最適化問題を前記求解装置に送り、

該求解装置は、送られた変換した最適化問題を解いて解yを求め、該求めた解yを前記解要求装置に送り、

該解要求装置は、送られた解yに対して、変数の逆変換$x=u^{-1}(y)$を行って元の最適化問題に対する解xを求め、該解xを出力することを特徴とする最適化問題の解取得方法。

【請求項３】　請求項２記載の最適化問題の解取得方法において、

前記最適化問題の等号制約条件がm行n列の係数行列Aおよびm次元右辺ベクトルbによって$Ax=b$と表現されている場合に、

前記変数変換として、n行n列の置換行列Qによる線形変換$y=Q^{-1}x$を用い、

前記式の同値変形として、m行m列の正則行列Pを該等号制約条件$Ax=b$の両辺に

出証特２００１－３０６５３７４

掛ける処理を用い、

前記変数の逆変換として、線形変換x=Qyを用いることを特徴とする最適化問題の解取得方法。

【請求項４】　請求項３記載の最適化問題の解取得方法において、

前記係数行列Aを縁付きブロック対角形式に変換するm行m列の左置換行列をP_1、n行n列の右置換行列をQ_1とし、

該P_1，Q_1を前記係数行列Aに作用させて得られる縁付きブロック対角行列P_1AQ_1において、各対角ブロック内部の行の間でのみ線形変換を行う行列をP_2、および各ブロック内部の列の間でのみ置換を行う行列をQ_2とするとき、前記正則行列Pとして行列P_2P_1を用い、置換行列Qとして行列Q_1Q_2を用いることを特徴とする最適化問題の解取得方法。

【請求項５】　ユーザからの最適化問題の求解要求を受け付ける少なくとも１台のクライアント計算機システムと、与えられた最適化問題に対する解を求めるサーバ計算機システムと、該各クライアント計算機システムを該サーバ計算機システムに接続するネットワークとを備える最適化問題の求解システムであって、

前記クライアント計算機システムは、

m行n列の係数行列Aとm次元右辺ベクトルbにより定義される等号制約条件Ax=b，不等号制約条件x≧0，最小化すべき目的関数f(x)によって表現された最適化問題の入力を受け付ける問題入力部と

暗号鍵を受け付ける暗号入力部と、

前記暗号入力部から入力された暗号鍵を用いてm行m列の正則行列Pおよびn行n列の置換行列Qを生成する変換行列生成部と、

該正則行列Pおよび該置換行列Qを用いて、前記最適化問題を異なる等号制約条件(PAQ)y=Pb，不等号制約条件y≧0，目的関数f(Qy)を持つ別の最適化問題に変換する問題変換部と、

変換した最適化問題を前記ネットワークを介して前記サーバ計算機システムに送る問題出力部と、

該サーバ計算機システムから受け取った変換後の最適化問題に対する解yに対

して逆変換x=Qyを行い、元の問題に対する解xを求める逆変換部を有することを特徴とする最適化問題の求解システム。

【請求項６】　少なくとも１台のクライアント装置と、最適化問題に対する解を求めるサーバ装置を有するシステムにおける求解サービス処理方法であって、

前記クライアント装置からのサービス開始要求に応じて前記サーバ装置は、

(1)m行n列の係数行列Aとm次元右辺ベクトルbにより定義される等号制約条件Ax=b，不等号制約条件x≧0，最小化すべき目的関数f(x)によって表現された最適化問題の入力をユーザから受け付ける問題入力機能と、

(2)ユーザからの暗号鍵を受け付ける暗号入力機能と、

(3)上記暗号入力機能により入力された暗号鍵を用いてm行m列の正則行列Pおよびn行n列の置換行列Qを生成する変換行列生成機能と、

(4)該正則行列Pおよび該置換行列Qを用いて、該最適化問題を異なる等号制約条件(PAQ)y=Pb，不等号制約条件y≧0，目的関数f(Qy)を持つ別の最適化問題に変換する問題変換機能と、

(5)変換後の最適化問題を外部装置に送信するために出力する問題出力機能と、

(6)変換した問題に対する解yを外部装置から受け取るための解入力機能と、

(7)解yに対して、上記(3)のステップで生成される行列Qを用いて逆変換x=Qyを行い、元の問題に対する解xを求める逆変換機能と、

(8)逆変換後の解xを出力する解出力機能とをコンピュータに実現させるプログラムを前記クライアント装置に送信し、

前記プログラムを受信したクライアント装置は、受信したプログラムの前記(1)，(2)，(3)，(4)，(5)の機能を実現して最適化問題を別の問題に変換して前記サーバ装置に送信し、

該サーバ装置は該受信した別の問題の解yを求め、該解yを前記クライアント装置に送信し、

該クライアント装置は、前記プログラムの前記(6)，(7)，(8)の機能を実現して元の最適化問題の解xを得ることを特徴とする求解サービス処理方法。

【請求項７】　少なくとも１台のクライアント装置と、最適化問題に対する解を求めるサーバ装置と、プログラム提供装置を有するシステムにおける求解サービス処理方法であって、

前記クライアント装置からのサービス開始要求に応じて前記サーバ装置は、プログラム提供装置を該クライアント装置に紹介し、

該クライアント装置は該プログラム提供装置にプログラムを要求し、

該プログラム提供装置は、

(1)m行n列の係数行列Aとm次元右辺ベクトルbにより定義される等号制約条件Ax=b，不等号制約条件x≧0，最小化すべき目的関数f(x)によって表現された最適化問題の入力をユーザから受け付ける問題入力機能と、

(2)ユーザからの暗号鍵を受け付ける暗号入力機能と、

(3)上記暗号入力機能により入力された暗号鍵を用いてm行m列の正則行列Pおよびn行n列の置換行列Qを生成する変換行列生成機能と、

(4)該正則行列Pおよび該置換行列Qを用いて、該最適化問題を異なる等号制約条件(PAQ)y=Pb，不等号制約条件y≧0，目的関数f(Qy)を持つ別の最適化問題に変換する問題変換機能と、

(5)変換後の最適化問題を外部装置に送信するために出力する問題出力機能と

、

(6)変換した問題に対する解yを外部装置から受け取るための解入力機能と、

(7)解yに対して、上記(3)のステップで生成される行列Qを用いて逆変換x=Qyを行い、元の問題に対する解xを求める逆変換機能と、

(8)逆変換後の解xを出力する解出力機能とをコンピュータに実現させるプログラムを前記クライアント装置に送信し、

前記プログラムを受信したクライアント装置は、受信したプログラムの前記(1)，(2)，(3)，(4)，(5)の機能を実現して最適化問題を別の問題に変換して前記サーバ装置に送信し、

該サーバ装置は該受信した別の問題の解yを求め、該解yを前記クライアント装置に送信し、

該クライアント装置は、前記プログラムの前記(6)，(7)，(8)の機能を実現し

て元の最適化問題の解xを得ることを特徴とする求解サービス処理方法。

【請求項８】　コンピュータに、

m行n列の係数行列Aとm次元右辺ベクトルbにより定義される等号制約条件Ax=b，不等号制約条件x≧0，最小化すべき目的関数f(x)によって表現された最適化問題の入力を受け付ける問題入力機能と、

暗号鍵を受け付ける暗号入力機能と、

上記暗号入力部から入力された暗号鍵を用いてm行m列の正則行列Pおよびn行n列の置換行列Qを生成する変換行列生成機能と、

該正則行列Pおよび該置換行列Qを用いて、該最適化問題を異なる等号制約条件(PAQ)y=Pb，不等号制約条件y≧0，目的関数f(Qy)を持つ別の最適化問題に変換する問題変換機能と、

変換後の最適化問題を出力する問題出力機能と、

変換した問題に対する解yを受け取る解入力機能と、

解yに対して、上記(3)のステップで生成される行列Qを用いて逆変換x=Qyを行い、元の問題に対する解xを求める逆変換機能と、

逆変換後の解xを出力する解出力機能とを実現させるプログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、処理装置が問題の求解を他の処理装置に依頼して問題の解を得る場合における機密保持に関する。

【０００２】

【従来の技術】

物流業、金融業などの産業分野では、トラックの配送経路の最適化、債券ポートフォリオの最適化をはじめとして、さまざまな最適化問題を解く必要がある。

例えば、トラックの配送経路の最適化では、地図上に複数の配送地点が与えられたとき、そのすべてを1回ずつ通り、長さが最小となる経路を求める。これにより、トラックの走行距離を可能な限り短くすることができ、運送に要する経費を最小化することができる。

例として、平面上に100個の配送地点が与えられたとき、これらをランダムな順で回ったときの配送経路を図２に、最適な配送経路を図３に示す。

ランダムな順での配送経路に比べ、最適な配送経路では走行距離が数分の１に小さくなっており、運送費用が大きく節約できる。

また例えば、債券ポートフォリオの最適化では、一定量の資金が与えられており、かつ株式、国債、社債などの各債券について、期待収益率と収益率の分散とが与えられているという条件の下で、資金を各債券にどのように分散投資すれば、全体の収益率を一定に保ちつつ、全体のリスクすなわち収益率の分散を最小化できるかという問題を解く。

【０００３】

これらの問題は、数学的には線形計画問題、二次計画問題、または混合型整数計画問題として定式化できる。

線形計画問題とは、等号制約条件$Ax=b$，不等号制約条件$x \geqq 0$の下で目的関数$c^t x$を最小化するxを求める問題である。

なお、ここでxは未知数のn次元ベクトルであり、Aはm行n列の定数行列、cはn次元の定数ベクトルである。また、$x \geqq 0$はxのすべての要素が非負であるという条件を表し、$c^t x$はベクトルcとベクトルxとの内積を表す。

二次計画問題とは、線形計画問題において、目的関数を二次間数$c^t x + x^t B x$に変えた最適化問題である。

ここで、Bはn行n列でかつ非負定値の定数行列である。

混合型整数計画問題とは、線形計画問題において、未知数ベクトルxの一部の成分に整数条件が課された最適化問題である。

【０００４】

上記のトラックの配送経路の最適化は、複数の配送地点のすべてを1回ずつ通るという条件を整数条件付きの等号制約条件$Ax=b$で表すことができ、配送経路の長さを一次関数$c^t x$で表すことができるため、混合型整数計画問題となる。

また、上記の債券ポートフォリオの最適化では、資金量一定および収益率一定という条件を等号制約条件$Ax=b$で表すことができ、リスク最小化のための目的関数を二次関数$x^t B x$で表すことができるため、二次計画問題となる。

【０００５】

以上の二つの例は、最適化を直接の目的とする例であるが、産業における最適化問題の応用はこれに留まらない。

たとえば金融業では、企業への融資におけるリスク管理のために、倒産の可能性が高い企業・低い企業を事前に推定する企業格付けを行う必要がある。

このための一つの方法として、最適化問題を利用する方法が提案されている（たとえば今野浩：「数理計画法による市場リスク／信用リスクの計量と管理」、平成12年度第4回ORセミナーテキスト「金融リスクとOR」、（社）日本オペレーションズ・リサーチ学会、参照）。

この方法では、(1) 融資の対象となる企業を自己資本比率、キャッシュフローなどの財務指標により高次元空間にプロットし、(2) 過去の実績を元に、この空間中で倒産企業・非倒産企業を最もよく判別できる（すなわち最も誤判別の少ない）超平面を計算し、(3) この超平面からの距離により対象企業の格付けを行う。

財務指標の空間と最適な平面の例を図４に示す。

図中の白丸3が非倒産企業、黒丸4が倒産企業を表し、直線5が判別超平面を表す。

この方法では、(2)のステップにおいて、判別のための最適な超平面を求めるために線形計画問題を用いる。同様の手法は、個人向けのクレジットカードの入会審査等にも使われる。このように、最適化問題の求解は、狭義の最適化を超えて、物流業や金融業のさまざまな場面で必要とされる技術となっている。

【０００６】

近年では、物流業における大規模サプライ・チェーン・マネジメントの普及、金融業における銀行合併などにより、上記のような応用で解くべき最適化問題も大規模化しており、スーパーコンピュータの利用が必要な例も増加しつつある。

そのため、各企業の所有する計算機資源のみでは求解が困難になっており、大規模なスーパーコンピュータを備えて複数の企業から最適化問題の求解を請け負うアプリケーション・サービス・プロバイダ（ASP）の出現が予想されている。

このようなASPの実用化に当たっての鍵は、機密保持のための対策である。

実際、最適化問題に関する情報は、物流業であれば配送地点や配送経路、金融業であれば債券ポートフォリオの内容、融資先の企業の財務指標、融資先企業の格付け情報、クレジットカード審査のための個人情報、審査結果など、業務の根幹に関わる機密情報を含む。

したがって、もしASPへの最適化の依頼によってこれらの情報が漏洩する恐れがあるとすれば、依頼を行うことは考えにくい。そのため、最適化問題の求解に関するASPを実用化するには、解くべき最適化問題の情報、得られた解の情報の両方について、十分な機密保持を保証できる方法が必要である。

【０００７】

このための方法としては、従来、たとえば特開平10-154136号公報「シミュレーションプログラムの実行支援方法およびプログラム割り当て方法」で提案されている方法が主に使われてきた。

この方法により機密保持を行う例を図５に示す。

この例では、解くべき最適化問題が格納されている顧客の計算機システム6と、求解を行うASPの計算機システム7とがネットワーク8で結ばれている。

顧客は、ASPに求解を依頼するに当たり、まず解くべき問題9をある暗号鍵10によって暗号化してビット列11に変換する。

次に、このビット列11及び暗号鍵10をネットワーク8経由でASP側に送信する。

ただし、暗号鍵を送るに当たっては、これを別の公開鍵方式の暗号で暗号化して送るなどの方法により、暗号鍵がネットワーク上で傍受されないように工夫することが必要である。

ASP側では、ビット列11および暗号鍵10を受け取り、復号化を行って元の問題を復元してから、それに対する解12を求め、それを再び暗号化してネットワーク8経由で顧客側に送り返す。

顧客側では解を復号化し、元の問題に対する解を得る。

この方法では、解くべき問題及び解を暗号化してネットワークで転送するため、ネットワーク上の情報を第三者が傍受しても、問題及び解に関する情報は得られない。

以上が従来法による機密保持方法である。

【０００８】

【発明が解決しようとする課題】

従来の機密保持方法では、ネットワーク上からの第三者の傍受に対して、解くべき問題と解の機密を保持することが可能である。しかし、この方法には２つの問題点がある。

第１の問題点は、ASPのような求解システム側で復号化を行うため、求解システム側に対しては解くべき問題と解の情報が完全に開示されてしまうことである。したがって、求解システム側に悪意を持つスタッフがいた場合、あるいは求解システムに侵入があった場合には、顧客の情報が漏洩する可能性がある。

第２の問題点は、求解システム側で復号化を行うために、暗号化された解くべき問題の情報に加え、暗号鍵も求解システム側に送らなければならないことである。通常、暗号鍵を送るに当たっては、別の公開鍵暗号によってこれを暗号化するなどの方法を取り、安全性を高める工夫を行うが、これは余計な手間を必要とし、また、公開鍵暗号が破られる可能性がゼロではないため、安全性の低下にもつながる。

本発明は上記２つの問題点を解決し、求解システムへの最適化問題の求解依頼において、求解システム側に解くべき問題と解の情報を渡さず、かつ暗号鍵をネットワーク上で送ることも不要とする、新しい機密保持の方法を提供することを目的とする。

【０００９】

【課題を解決するための手段】

上記目的を達成するため、本発明では、

入力された問題に対する解を要求する解要求装置から求解装置に問題を送り、求解装置で問題の解を求め解要求装置に送り、解要求装置で解を出力して問題の解を得る場合に、解要求装置は、入力された問題を暗号鍵により暗号化し、該暗号化した問題を求解装置に送り、求解装置は、送られた暗号化した問題を暗号化したままの状態で解いて解を求め、該求めた解を解要求装置に送り、解要求装置は、送られた解を暗号鍵により復号化し、復号化した解を出力するようにしている。

入力された最適化問題に対する解を要求する解要求装置から求解装置に問題を送り、求解装置で最適化問題の解を求め解要求装置に送り、解要求装置で解を出力して最適化問題の解を得る場合に、

解要求装置は、適当に定めた変数変換y=u(x)および式の同値変形によって、該最適化問題を異なる等号制約条件g'（y)=0，不等号制約条件h'（y)≧0，目的関数f'（y)を持つ別の最適化問題に変換し、該変換した最適化問題を前記求解装置に送り、求解装置は、送られた変換した最適化問題を解いて解yを求め、求めた解yを解要求装置に送り、解要求装置は、送られた解yに対して、変数の逆変換$x=u^{-1}(y)$を行って元の最適化問題に対する解xを求め、解xを出力するようにしている。

【００１０】

【発明の実施の形態】

以下、本発明の原理および実施例１を、図面により詳細に説明する。

ここで実施例として挙げるのは、ユーザから最適化問題の求解要求を受け付けるクライアント計算機システムと、与えられた最適化問題に対する解を求めるサーバ計算機システムと、各クライアントをサーバに接続するネットワークとを備え、元の最適化問題の情報およびその解に関する情報ををサーバ側に与えることなく、クライアントからサーバへの最適化問題の求解依頼をし、サーバにおいて求解依頼された問題の解を求め、求めた解をサーバからクライアントに返送し、クライアントにおいて解を出力することを可能とするシステムである。

【００１１】

図１に本発明の機密保持方法の概要を、問題の求解を依頼する顧客とASPとの間での機密保持の場合を例として示す図である。

顧客の計算機システム6では、解くべき問題9を暗号鍵10を用いて暗号化し、暗号化した解くべき問題11をネットワーク8を介してASPの計算機システム7に送る。

ASPの計算機システム7は問題を解いて解yを求め、ネットワーク8を介して顧客の計算機システム6に送る。

顧客の計算機システム6は解yを暗号鍵10を用いて復号化して解xを求める。

ASP側は変換された問題「minimize $f^t y$ s.t. Dy=e, y≧0」のみを扱うため、元の問題に関する情報を得ることはない。また、元の問題から別の問題への変換は同値変形であるため、変換された問題の解から元の問題の解を求めることが可能である。

【００１２】

本システムの構成図を図６に示す。

クライアント計算機システム13は、入力装置14と出力装置15に加えて

(1)m行n列の係数行列Aとm次元右辺ベクトルbにより定義される等号制約条件Ax=b，不等号制約条件x≧0，最小化すべき目的関数f(x)によって表現された最適化問題の入力を受け付ける問題入力部16、

(2)機密保持のための暗号鍵を受け付ける暗号入力部17、

(3)上記暗号入力部から入力された暗号鍵10を用いてm行m列の正則行列Pおよびn行n列の置換行列Qを生成する変換行列生成部18、

(4)正則行列Pおよび該置換行列Qを用いて、該最適化問題を異なる等号制約条件(PAQ)y=Pb，不等号制約条件y≧0，目的関数f(Qy)を持つ別の最適化問題に変換する問題変換部19、

(5)変換後の最適化問題をネットワーク8を通じてサーバに送信する問題出力部20、

(6)変換後の問題に対する解yをネットワーク8を通じてサーバから受け取る解入力部21、

(7)解yに対して、上記(3)のステップで生成される行列Qを用いて逆変換x=Qyを行い、元の問題に対する解xを求める逆変換部22、

(8)逆変換後の解xを出力する解出力部23、

から構成される。なお、PAQはPとAとQの乗算を示し、QyはQとyの乗算を示す。

【００１３】

サーバ計算機システム24は、

(9)変換後の最適化問題をネットワーク8を通じてクライアントから受け取る問題入力部25、

(10)この問題に対する解を求める求解部26、

(11)求めた解をネットワーク8を通じてクライアントに送信する解出力部27から構成される。

【００１４】

本実施例におけるクライアント側の処理を図７に、サーバ側の処理を図８に示す。

クライアントは、まずユーザから最適化問題の入力を受け付け、入力された問題サイズn，m，係数行列A，右辺ベクトルb，目的関数f(x)を問題入力部に格納する（処理29）。

次に、クライアントはユーザから暗号鍵の入力を受け付け、これを暗号入力部に格納する（処理30）。

次に変換行列生成部において、この暗号鍵を用いてm行m列の正則行列Pおよびn行n列の置換行列Qを生成する（処理31）。

行列PおよびQの生成方法の詳細は後に述べる。

次に問題変換部において、置換行列Qによる解の線型変換$y=Q^{-1}x$、および正則行列Pを等号制約条件Ax=bの両辺に掛ける変換を行い、与えられた問題を、異なる等号制約条件Dy=e、不等号制約条件$y \geqq 0$、目的関数g(y)を持つ同値な最適化問題に変換する（処理32）。

なお、以上の説明より、行列D，ベクトルe，関数gは、それぞれ計算式D=PAQ，e=Pb，g(y)=f(Qy)により与えられることが明らかである。

次にクライアントは、変換した問題を問題出力部に格納し、ネットワークを通じてサーバに送信する（処理33）。

なお、クライアントがサーバに送信するのは変換後の問題のみであり、変換に使った暗号鍵、および行列P，Qは送信しない。

【００１５】

次にサーバは、ネットワークを通じてクライアントから変換後の最適化問題を受け取り（処理39）、それを問題入力部に格納し、求解部においてその解yを求める（処理40）。

ここで解を求めるのに用いる方法は、最適化問題の種類に応じて、既存の任意の解法を用いればよい。

たとえば線形計画問題の場合は単体法、二次計画問題の場合は逐次二次計画法などが利用できる。

これらの解法の詳細については、たとえば今野浩、山下浩著：「非線形計画法」、日科技連出版社、1987.を参照。

解yを求めた後、サーバはこれを解出力部に格納し、ネットワークを通じてクライアントに送信する（処理41）。

【００１６】

次にクライアントは、ネットワークを通じてクライアントから変換後の最適化問題の解yを受け取り、解入力部に格納する（処理34）。

次に逆変換部において、上記の行列Qを用いてこの解に対して逆変換x=Qyを行い、元の問題に対する解xを求めて解出力部に格納する（処理35）。

なお、ここで用いる行列Qは、最適化問題の変換時に作成した行列を取っておいて用いてもよいし、暗号鍵をもう一度ユーザに入力させ、それを用いて変換行列生成部においてもう一度生成してもよい。

最後にクライアントは、元の問題の解xを解出力部より出力し（処理36）、処理を終了する。

【００１７】

以上の処理のうち、暗号鍵よりm行m列の正則行列Pおよびn行n列の置換行列Qを生成する変換行列生成部の処理の一例を図９に示す。

変換行列生成部では、第１のステップとして、元の問題の係数行列Aを縁付きブロック対角行列に変換するm行m列の左置換行列P_1、n行n列の右置換行列Q_1を生成する（処理44）。

ここで縁付きブロック対角行列とは、行列を縦横に4個のブロックに分割したとき、左上のブロックについては内部に複数の対角ブロックが存在し、ゼロでない要素がこの複数の対角ブロック内部にのみ存在するような行列である。

なお、左上以外のブロックについては、ゼロでない要素はブロック中のどこにあってもよい。

元の係数行列Aの非ゼロ要素のパターンを図１０に示す。

57が係数行列、58が非ゼロ要素を示す。

また、Aに左からP_1、右からQ_1を掛けて得られる縁付きブロック対角行列P_1AQ_1の非ゼロ要素のパターンを図１１に示す。

60が左上のブロック、61が対角ブロックを示す。

任意の行列は左置換行列と右置換行列によって縁付きブロック対角行列に変形できることが知られており、具体的にはNested Dissection法と呼ばれる方法を用いることにより、P_1とQ_1が計算できる。

これらの点に関する詳細は、たとえばK. A. Gallivan他著：" Parallel Algorithms for Matrix Computation"，SIAM，1990を参照されたい。

【００１８】

次に、第２のステップとして、暗号鍵を用いて、各ブロックの中で左から線型変換を行う行列P_2および右から置換を行う行列Q_2を生成する。

いま、暗号鍵が6N個の乱数の列として与えられているとする。

このとき、まず第１の乱数を用いて行列P_1AQ_1の行を１つ選び（処理46）、第２の乱数を用いてそれと同じ対角ブロック内にある別の行を１つ選ぶ（処理47）。

選んだ第１の行を第L_1行、第２の行を第L_2行とする。

次に、第３と第４の乱数r，sを用いて、m行m列の単位行列の第（L_1，L_2）成分にr、第（L_2，L_1）成分にsを加えた行列P_1'を生成する（処理48）。

この行列P_1'を行列P_1AQ_1に左から掛けることは、行列P_1AQ_1の第L_1行に第L_2行のr倍を加え、第L_2行に第L_1行のs倍を加えることと等価である。

次に、第５の乱数を用いて行列P_1AQ_1の列を１つ選び（処理49）、第６の乱数を用いてそれと同じ対角ブロック内にある別の列を１つ選ぶ（処理50）。

選んだ第１の列を第R_1列、第２の列を第R_2列とするとき、n行n列の単位行列の第（R_1，R_1）成分と第（R_2，R_2）成分とをゼロとし、第（R_1，R_2）成分と第（R_2，R_1）成分とを１とした行列Q_1'を生成する（処理51）。

この行列Q_1'を行列P_1AQ_1に右から掛けることは、行列P_1AQ_1の第R_1列と第R_2列とを入れ替えることと等価である。

このようにして、暗号鍵の最初の６個の乱数を用いてP_1'とQ_1'とを生成し、以後、暗号鍵中の乱数を順に用いて、同様にP_2'，Q_2'，P_3'，Q_3'，…，P_N

’，Q_N’を生成する（処理45）。

これらを用いて、$P_2 = P_N' \cdots P_2' P_1'$，$Q_2 = Q_1' Q_2' \cdots Q_N'$により、行列$P_2$と行列$Q_2$とを生成する（処理52、53）。

【００１９】

最後に、第３のステップとして$P = P_2P_1$、$Q = Q_1Q_2$により、m行m列の正則行列Pおよびn行n列の置換行列Qを生成する（処理54、55）。

【００２０】

ここで述べたPとQの生成法は、次のような３つの利点を持つ。

第１に、行列を縁付きブロック対角形式に変換した後に、対角ブロックの内部のみで、ある行に他の行の定数倍を加えたり、列を入れ替える処理を行うため、対角ブロック以外のゼロ要素のブロックは、この操作の影響を受けずにゼロ要素のブロックのままに留まる。

そのため、暗号化のための変換によって係数行列の非ゼロ用素数が大幅に増えることはない。

最適化問題を解くための計算量は係数行列の非ゼロ要素が多いほど増加するので、このことは暗号化によって最適化問題を解くための演算量が大幅に増えることはないことを意味する。

第２に、対角ブロックの中では任意に変換が可能であるため、変換の自由度は十分大きい。

このことは、変換された問題から元の問題を推定するのが困難であることを意味し、このPとQの生成法を用いた暗号化が十分な強度を持つことを保証する。

第３に、係数行列の変換は、ある行に他の行の定数倍を加える処理と列を入れ替える処理という単純な処理の組み合わせによって行われるため、変換のための計算量は十分小さい。

そのため、暗号化を行うためのオーバーヘッドは十分小さい。

以上のべたような利点のため、本実施例では上記のようなPとQの生成法を採用したが、本発明では、Pがm行m列の正則行列、Qがn行n列の置換行列という条件を満たしさえすれば、他の生成法で作った行列であっても、変換行列として利用することが可能である。

以上で、本発明の実施例を詳細に述べたが、本発明のメリットは大きく分けて２つある。

第１は、サーバ側は変換された問題のみを受け取り、ユーザが入力した元の問題、あるいは元の問題を復元するための暗号鍵、変換行列P，Qなどを受け取らないという点である。したがって、サーバ側は元の問題に対する情報を得ることができない。

このため、本発明の方式を利用すれば、サーバ側にも元の最適化問題に関する情報を開示したくないような極めて機密性の高い問題に関しても、求解の依頼が可能となる。

また、サーバの運営者に悪意を持つ者がいた場合、サーバに侵入があった場合などにおいても、ユーザの問題に関する情報が漏れることを防ぐことができる。

第２のメリットは、サーバに暗号鍵を渡す必要がないので、ネットワークを介して暗号鍵を送らなくて済むという点である。

通常、暗号鍵を送るに当たっては、別の公開鍵暗号によってこれを暗号化するなどの方法を取り、安全性を高める工夫を行うが、本発明ではこのような手間が不要の上、公開鍵暗号が破られることによる安全性の低下も防ぐことができる。

【００２１】

なお、本実施例ではクライアントが1台の場合を例に取って述べたが、本発明は複数台のクライアントがネットワークを通じてサーバに接続されている場合にも適用できることは明らかである。

また、本実施例では、クライアントとサーバとがネットワークを通じて情報の送受信を行う場合を例に取ったが、本発明は、情報がフロッピーディスク、磁気テープなどの記録媒体を通じてやり取りされる場合にも適用できることは明らかである。

また、本実施例では、最適化問題の等号制約条件が$Ax=b$、不等号制約条件が$x \geqq 0$という形をしている場合を例に取ったが、変数変換と式の同値変形とを組み合わせて最適化問題を別の最適化問題に変換するという本発明の原理は、より一般の等号制約条件$g(x)=0$、不等号制約条件$h(x) \geqq 0$を持つ最適化問題に対しても適用できる。

また、本実施例では、最適化問題の解を求める場合について説明したが、最適化問題以外の問題の解を求める場合にも適用できる。例えば、連立１次方程式の解を求める場合に適用できる。

最後に、本実施例では変換した問題をそのままネットワークを通じてクライアントからサーバに送信する場合を例に取ったが、従来の暗号化技術を用い、本発明の方法で変換した問題に対して更に暗号化を行ってから、それを暗号鍵と共にサーバに送ることにより、ネットワーク上での情報の安全性を更に高めることも可能である。

【００２２】

次に、本発明の第２の実施例を説明する。

本実施例は、求解装置（サーバ）が、本発明の方法による暗号化の変換プログラムをユーザに提供し、このプログラムを用いてユーザ（クライアント）に最適化問題を別の問題に変換させてからそれを受け取り、それに対する解を求めてユーザに提供し、ユーザ側で解の復号化を行わせることにより、求解装置側では暗号化前のユーザの最適化問題およびその解についての情報を得ることなしに、求解を行う求解サービス処理方法である。

本求解サービス処理方法は、実施例１の図６と同じクライアント、サーバ、ネットワークを備えたシステム上で実現される。

本実施例におけるクライアントおよびサーバの処理を図１２に示す。

クライアントは、まずサーバにサービスの開始要求を出す（処理63）。

サーバはこれを受け取り（処理73）、本発明の方法による暗号化の変換プログラムをクライアントに送信する（処理74）。

クライアントはこの変換プログラムを受け取る（処理64）。

次にクライアントはユーザから最適化問題の入力を受け付け（処理65）、暗号化変換のための暗号鍵の入力も受け付ける（処理66）。

その後、この暗号鍵を用いて、処理64で入手した変換プログラムにより、入力された最適化問題を同値な別の問題に変換する（処理67）。なお、この変換の詳細は、第１の実施例に述べた通りである。

こうして変換した最適化問題をサーバに送信する（処理68）。

サーバでは、変換後の最適化問題を受け取り（処理75）、解を求めて（処理76）、それをクライアントに送信する（処理77）。

クライアントは解を受け取り（処理69）、逆変換を行って元の問題の解を求め（処理70）、求めた解を出力する（処理71）。

以上により、サーバ側は、ユーザの入力した元の問題およびその解に関する情報を得ることなく、最適化問題の求解サービスを行うことが可能となる。

なお、本実施例では、クライアントが最初にサーバにサービス開始要求を出し、これに応えてサーバが暗号化用の変換プログラムを送信するが、本サービスを２回目以降に利用する場合には、このステップはなくてもよい。

また、クライアントは最初にユーザから最適化問題の入力を受け付け、その後にサーバにサービス開始要求を出して変換プログラムを受け取ってもよい。

【００２３】

次に、本発明の第３の実施例を説明する。

本実施例は、求解装置（サーバ）が、本発明の方法による暗号化の変換プログラムを指定して第三者であるプログラム提供者からユーザ（クライアント）に入手させ、このプログラムを用いてユーザに最適化問題を別の問題に変換させてからそれを受け取り、それに対する解を求めてユーザに提供し、ユーザ側で解の復号化を行わせることにより、求解装置側ではユーザの最適化問題およびその解についての情報を得ることなしに、求解を行う求解サービス処理方法である。

本求解サービス処理方法サービスは、実施例１の図６と同じクライアント、サーバ、ネットワーク、およびそれに加えて暗号化用の変換プログラムを提供するプログラム提供者からなるシステム上で実現される。

本実施例におけるクライアント、サーバ、およびプログラム提供者の処理を図１３に示す。

クライアントは、まずサーバにサービスの開始要求を出す（処理63）。

サーバはこれを受け取り（処理73）、本発明の方法による暗号化の変換プログラムの提供者をクライアントに紹介する（処理81）。

クライアントはこの紹介を受け（処理78）、プログラム提供者に対して、変換用プログラムを送信するよう依頼する（処理79）。

プログラム提供者はこの依頼を受け（処理82）、プログラムをクライアントに送信する（処理83）。

クライアントはこの変換プログラムを受け取る（処理80）。

クライアントが変換用プログラムを入手した後のクライアントおよびサーバの処理は、実施例２と全く同様である。

本実施例の場合でも、サーバ側は、ユーザの入力した元の問題およびその解に関する情報を得ることなく、最適化問題の求解サービスを行うことが可能となる。

【００２４】

なお、本実施例におけるサービス開始要求のクライアントからサーバへの送信、プログラム提供者のサーバからクライアントへの紹介などは、クライアントがサーバのホームページにアクセスすることを通じて行ってもよい。

この場合の画面例を図１４に示す。

この例では、サーバのホームページ84に初めてのユーザ用の入口85と登録済みのユーザ用の入口88が設けられている。

初めてのユーザは、まず入口85をクリックしてユーザ登録画面に飛び、そこでユーザ登録を行う。

次に、再び画面84画面い戻り、今度は暗号化の変換プログラム入手のためのリンク86をクリックする。

このリンクは変換プログラム提供者のホームページに接続されており、ユーザはそこから変換プログラムを入手できる。

以後の処理は、実施例２の場合と同様である。

一方、既にこのサービスを利用し、変換プログラムを入手済みのユーザは、登録済みのユーザ用の入口88をクリックして直接サービスメニューに飛べばよい。

なお、ホームページ上には暗号化プログラムの説明へのリンク87を設け、その先で本発明による暗号化の仕組みと利点について説明してもよい。

また、本例では初めてのユーザ用の入口、変換プログラム入手のためのリンク、登録済みのユーザ用の入口が１つのページに載っているが、これらは複数のページに分散配置されていてもよい。

【００２５】

【発明の効果】

以上述べたように、本発明では、サーバ側は変換された問題のみを受け取り、元の問題に対する情報を得ることができないため、サーバ側に元の最適化問題に関する情報を開示したくないような極めて機密性の高い問題に関しても、求解の依頼が可能となる。

また、サーバの運営者に悪意を持つ者がいた場合、サーバに侵入があった場合などにおいても、ユーザの問題に関する情報が漏れることを防ぐことができる。

また、ネットワークを介して暗号鍵を送らなくて済むため、暗号鍵を送るに当たって別の公開鍵暗号によってこれを暗号化するなどの手間が不要であり、公開鍵暗号が破られることによる安全性の低下も防ぐことができる。

【図面の簡単な説明】

【図１】

本発明の機密保持方法の概要を説明するための図である。

【図２】

ランダムな順でのトラックの配送経路を示す図である。

【図３】

最適なトラックの配送経路を示す図である。

【図４】

財務指標の空間と倒産・非倒産企業の判別平面を示す図である。

【図５】

従来の技術を用いた機密保持方法を示す図である。

【図６】

本発明の実施例を実行すべき計算機システムの例を示す図である。

【図７】

本実施例におけるクライアントの処理のフローチャートを示す図である。

【図８】

本実施例におけるサーバの処理のフローチャートを示す図である。

【図９】

変換行列生成部の処理の一例のフローチャートを示す図である。

【図１０】

係数行列Aの非ゼロ要素のパターンの例を示す図である。

【図１１】

縁付きブロック対角行列P_1AQ_1の非ゼロ要素のパターンの例を示す図である。

【図１２】

第２の実施例におけるクライアントおよびサーバの処理のフローチャートを示す図である。

【図１３】

第３の実施例におけるクライアント、サーバ、およびプログラム提供者の処理のフローチャートを示す図である。

【図１４】

プログラム提供者のホームページの画面例を示す図である。

【符号の説明】

１　配送地点

２　配送経路

３　非倒産企業

４　倒産企業

５　判別超平面

６　顧客の計算機システム

７　ASPの計算機システム

８　ネットワーク

９　解くべき問題

１０　暗号鍵

１１　ビット列

１２　解

１３　クライアント計算機システム

１４　入力装置

１５　出力装置

１６　問題入力部

１７　暗号入力部

１８　変換行列生成部

１９　問題変換部

２０　問題出力部

２１　解入力部

２２　逆変換部

２３　解出力部

２４　サーバ計算機システム

２５　問題入力部

２６　求解部

２７　解出力部

５７　係数行列A

５８　非ゼロ要素

５９　縁付きブロック対角行列P_1AQ_1

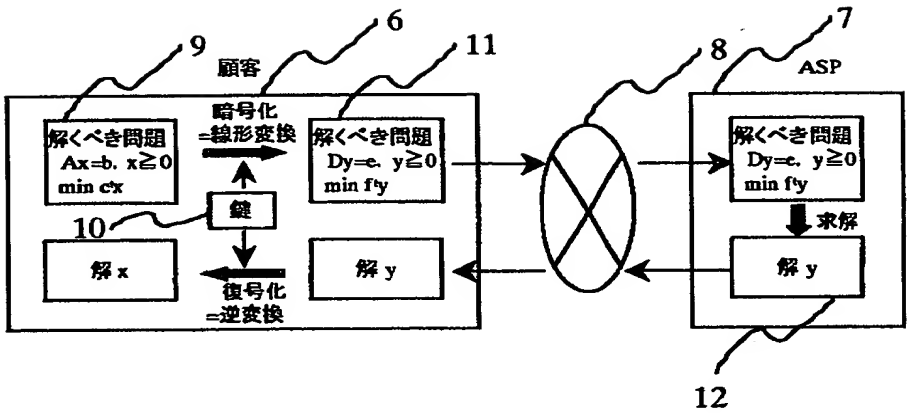
６０　左上のブロック

６１　対角ブロック

【書類名】　図面

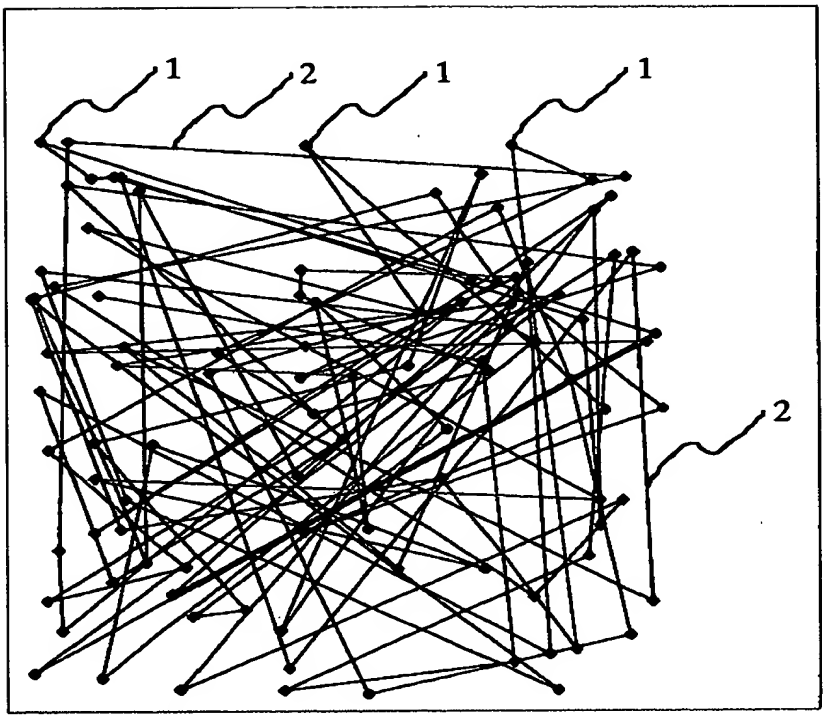
【図１】

図1


9
6
11
8
7
顧客
ASP
暗号化
=線形変換
解くべき問題
Ax=b, x≧0
min cx
解くべき問題
Dy=e, y≧0
min f'y
解くべき問題
Dy=e, y≧0
min f'y
鍵
10
求解
解 x
解 y
解 y
復号化
=逆変換
12

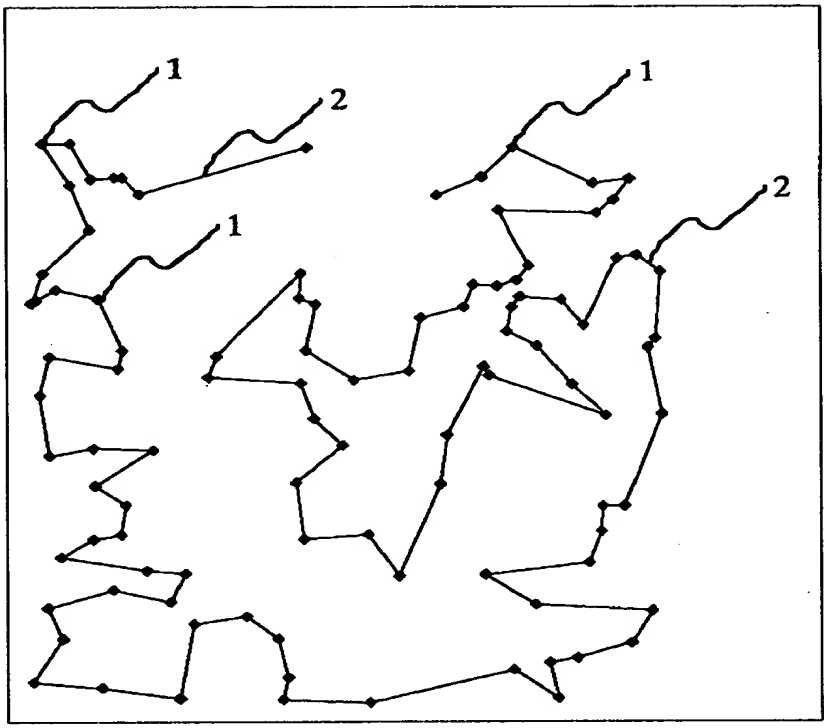
【図２】

図2



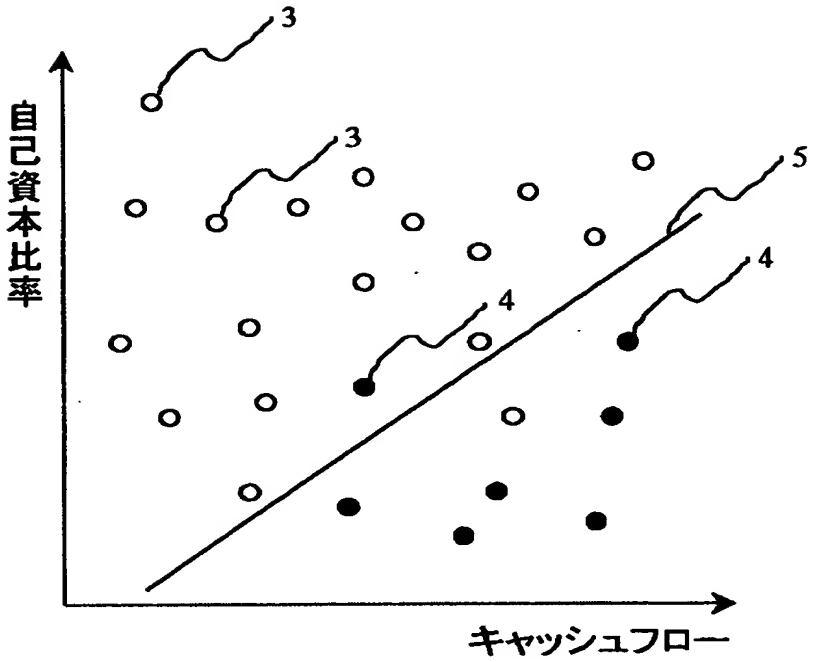
【図３】

図3



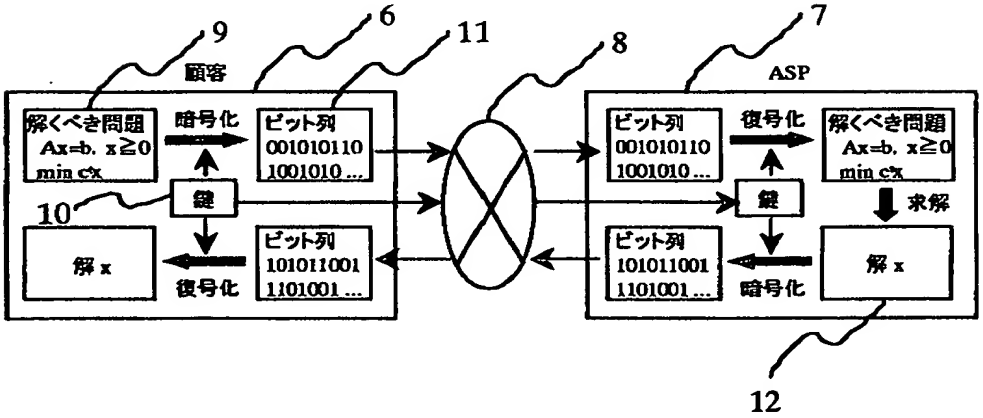
【図４】

図4


3
3
5
4
4
自己資本比率
キャッシュフロー

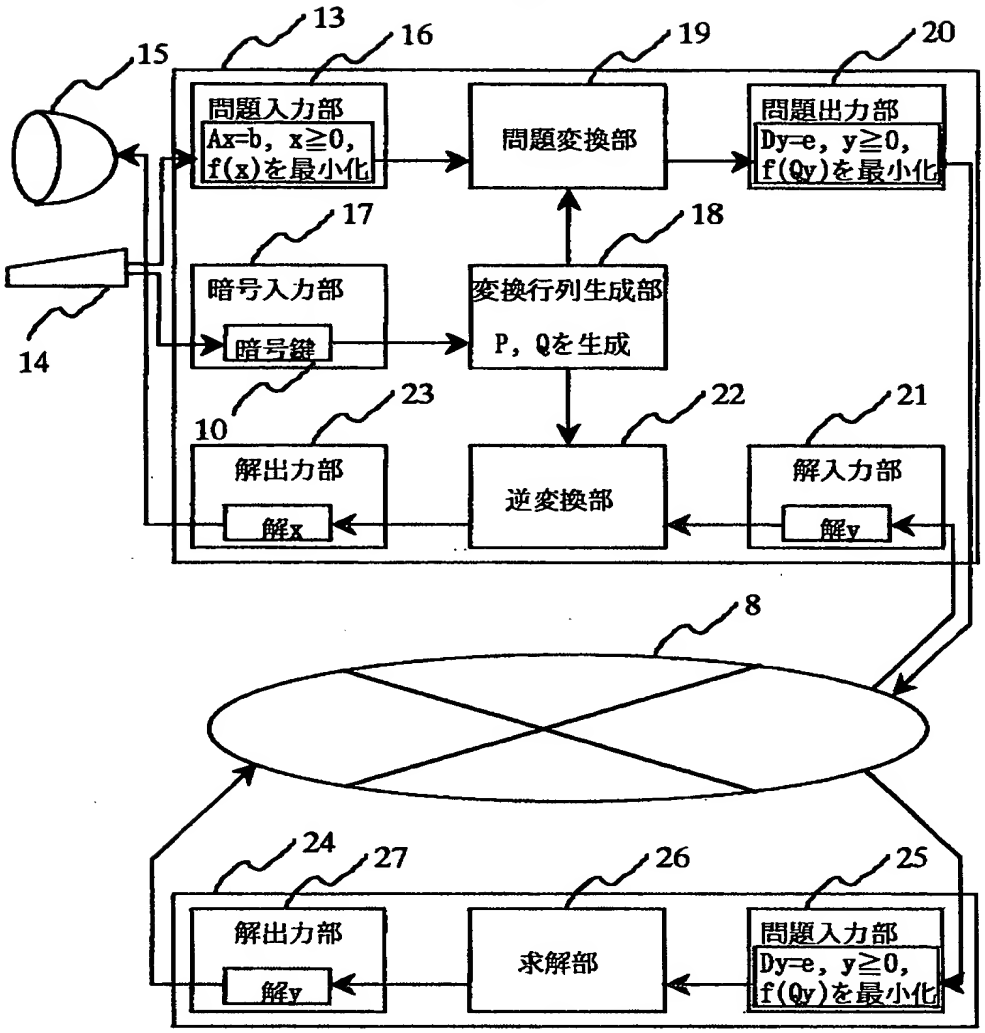
【図５】

図5


9
顧客
6
11
8
7
ASP
解くべき問題
Ax=b, x≧0
min cx
暗号化
ビット列
001010110
1001010 ...
鍵
10
解 x
ビット列
101011001
1101001 ...
復号化
ビット列
001010110
1001010 ...
復号化
解くべき問題
Ax=b, x≧0
min cx
鍵
求解
ビット列
101011001
1101001 ...
暗号化
解 x
12

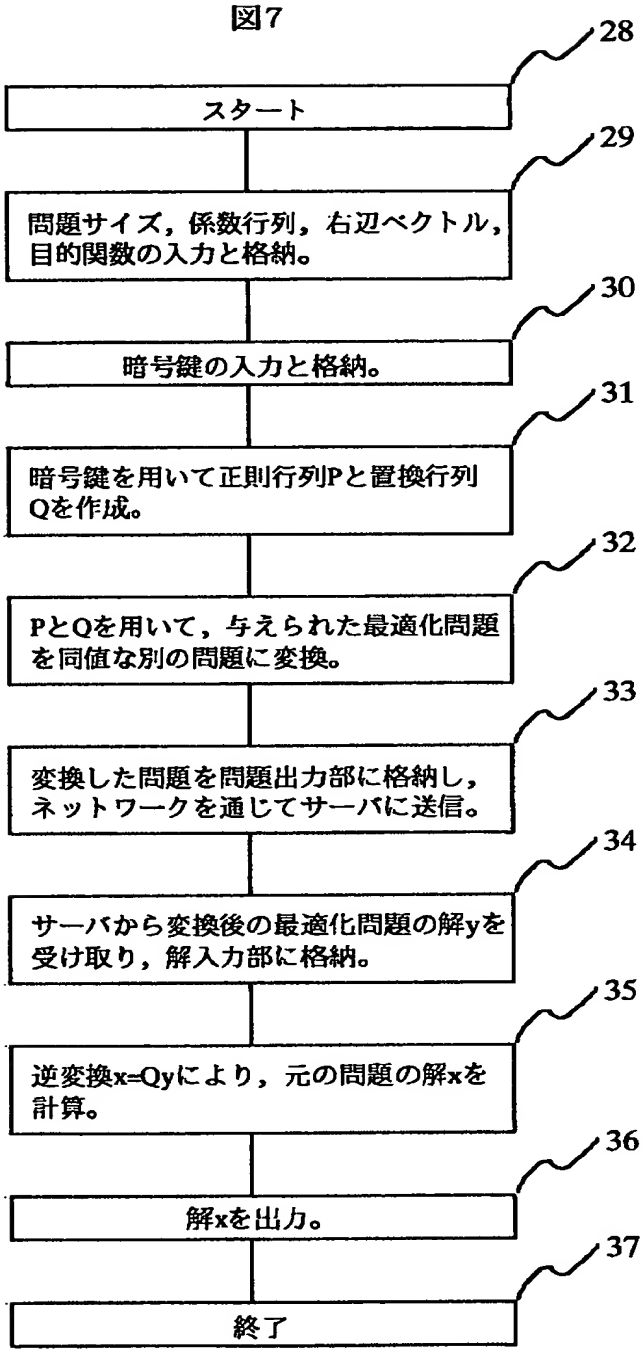
【図６】

図6


13
16
19
20
15
問題入力部
Ax=b, x≧0,
f(x)を最小化
問題変換部
問題出力部
Dy=e, y≧0,
f(Qy)を最小化
17
18
暗号入力部
暗号鍵
変換行列生成部
P, Qを生成
14
10
23
22
21
解出力部
解x
逆変換部
解入力部
解y
8
24
27
26
25
解出力部
解y
求解部
問題入力部
Dy=e, y≧0,
f(Qy)を最小化

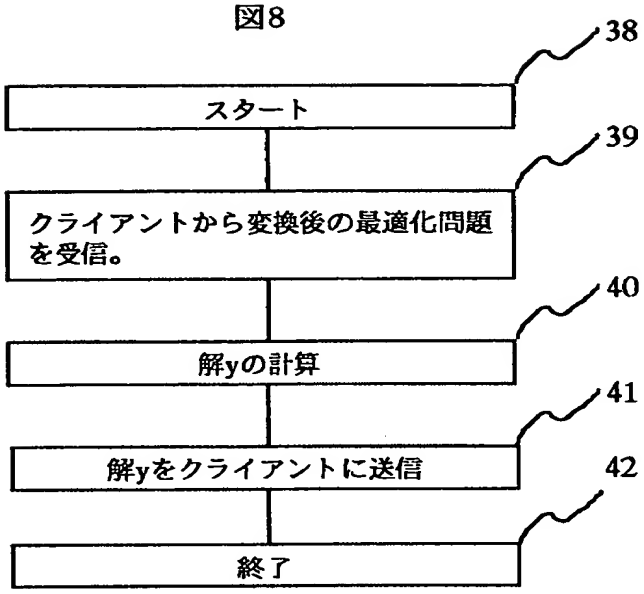
【図７】

図7


28
スタート
29
問題サイズ，係数行列，右辺ベクトル，目的関数の入力と格納。
30
暗号鍵の入力と格納。
31
暗号鍵を用いて正則行列Pと置換行列Qを作成。
32
PとQを用いて，与えられた最適化問題を同値な別の問題に変換。
33
変換した問題を問題出力部に格納し，ネットワークを通じてサーバに送信。
34
サーバから変換後の最適化問題の解yを受け取り，解入力部に格納。
35
逆変換x=Qyにより，元の問題の解xを計算。
36
解xを出力。
37
終了

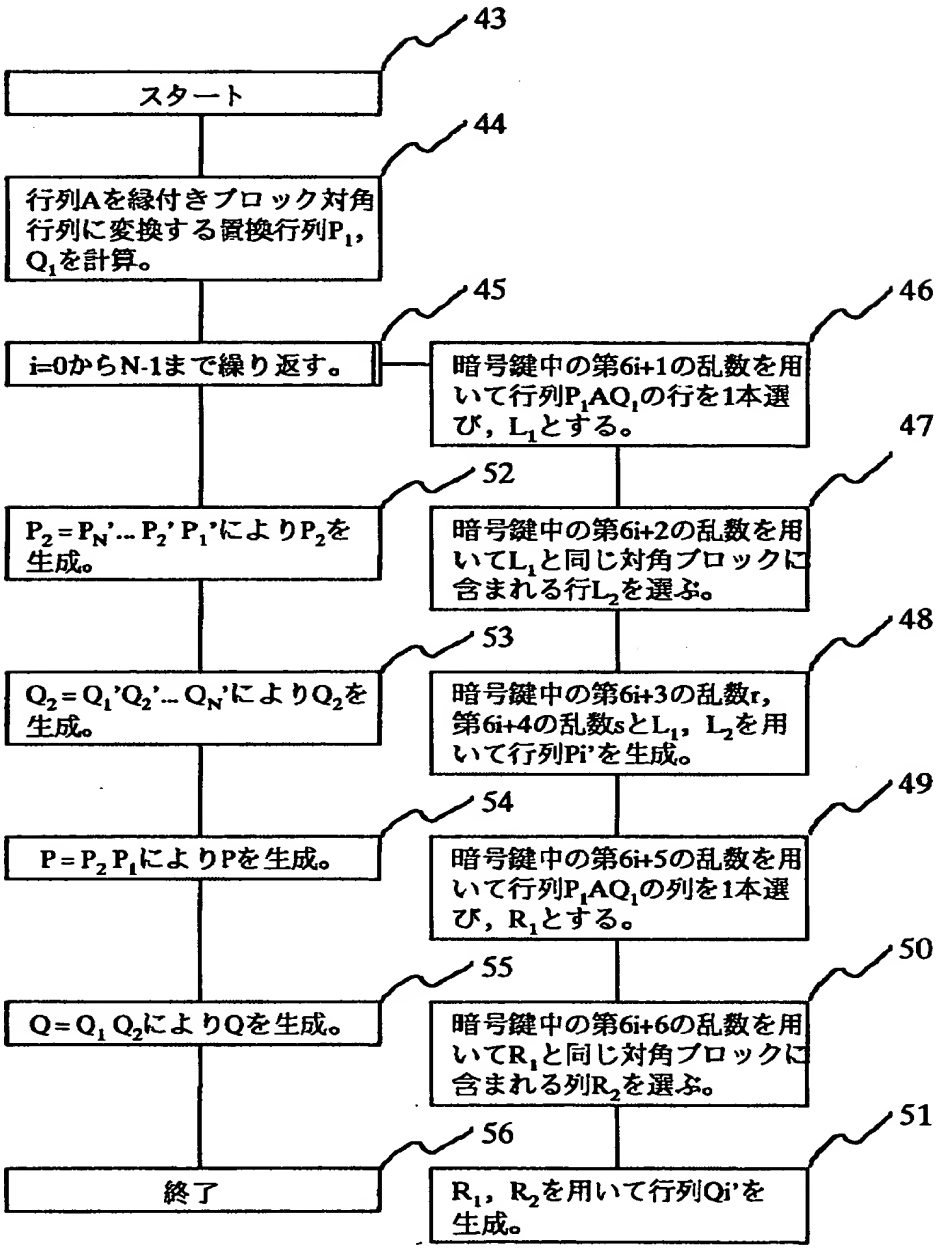
【図８】

図8


38
スタート
39
クライアントから変換後の最適化問題を受信。
40
解yの計算
41
解yをクライアントに送信
42
終了

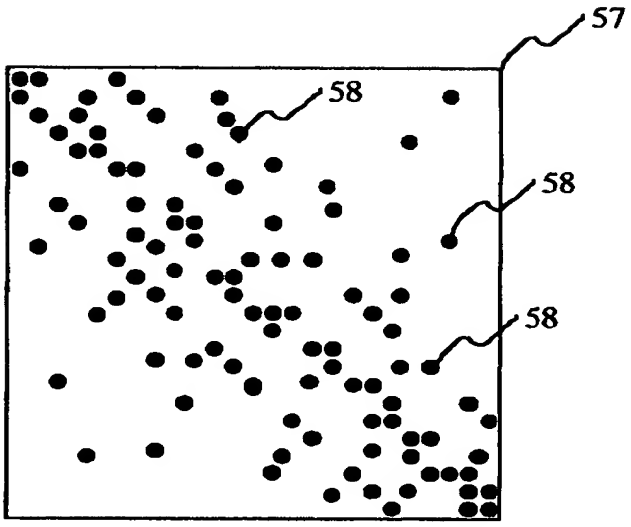
【図９】

図9


43
スタート
44
行列Aを縁付きブロック対角行列に変換する置換行列P_1, Q_1を計算。
45
i=0からN-1まで繰り返す。
46
暗号鍵中の第6i+1の乱数を用いて行列P_1AQ_1の行を1本選び，L_1とする。
47
暗号鍵中の第6i+2の乱数を用いてL_1と同じ対角ブロックに含まれる行L_2を選ぶ。
48
暗号鍵中の第6i+3の乱数r，第6i+4の乱数sとL_1，L_2を用いて行列Pi'を生成。
49
暗号鍵中の第6i+5の乱数を用いて行列P_1AQ_1の列を1本選び，R_1とする。
50
暗号鍵中の第6i+6の乱数を用いてR_1と同じ対角ブロックに含まれる列R_2を選ぶ。
51
R_1，R_2を用いて行列Qi'を生成。
52
$P_2=P_N'\cdots P_2'P_1'$によりP_2を生成。
53
$Q_2=Q_1'Q_2'\cdots Q_N'$によりQ_2を生成。
54
$P=P_2P_1$によりPを生成。
55
$Q=Q_1Q_2$によりQを生成。
56
終了

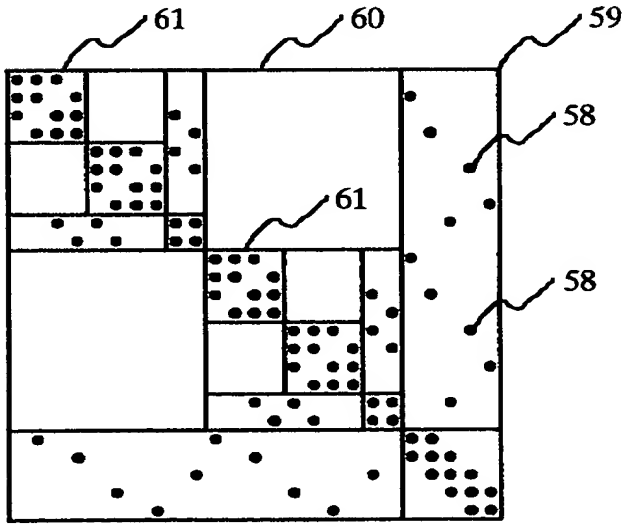
【図１０】

図10



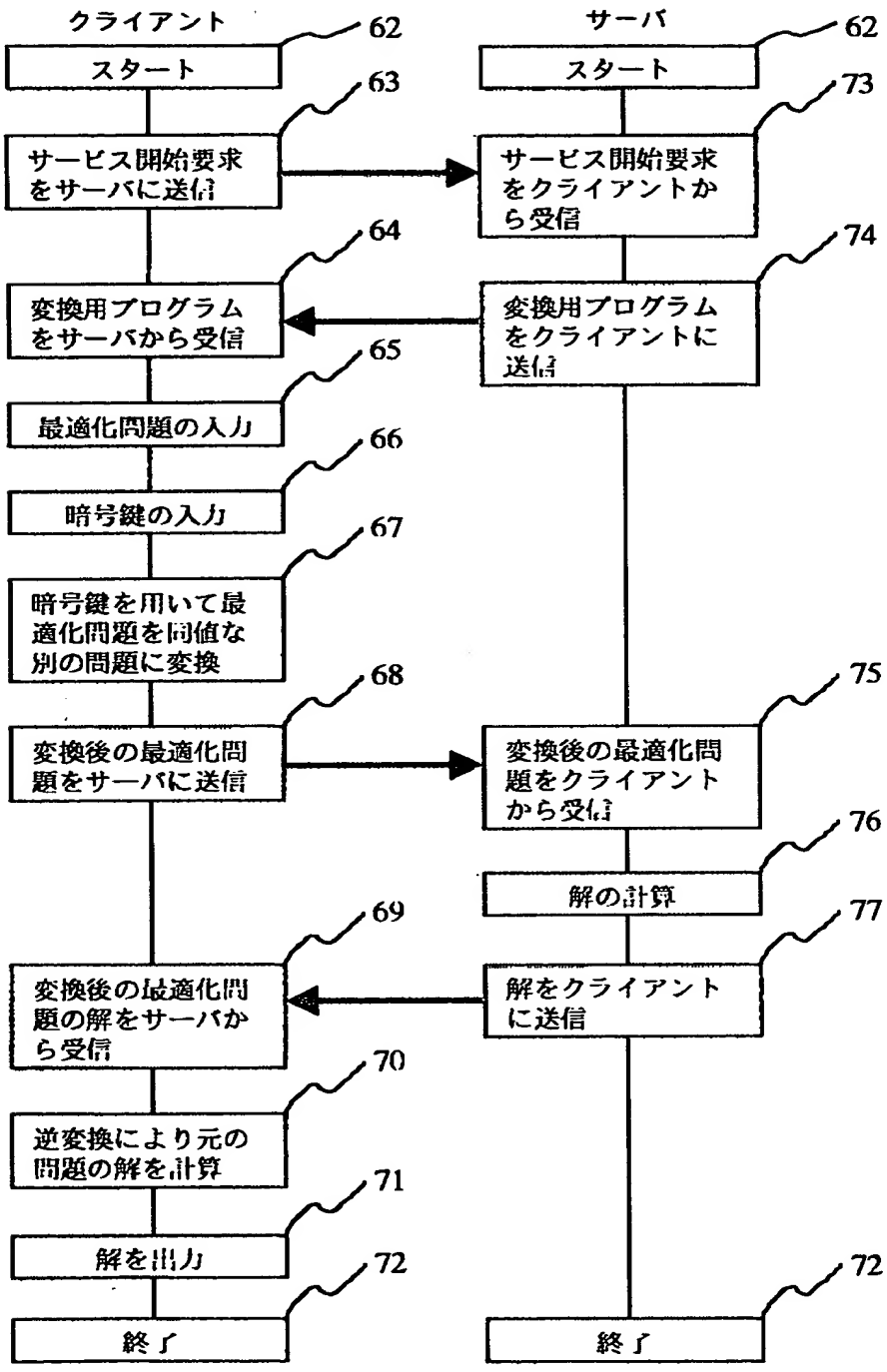
【図１１】

図11



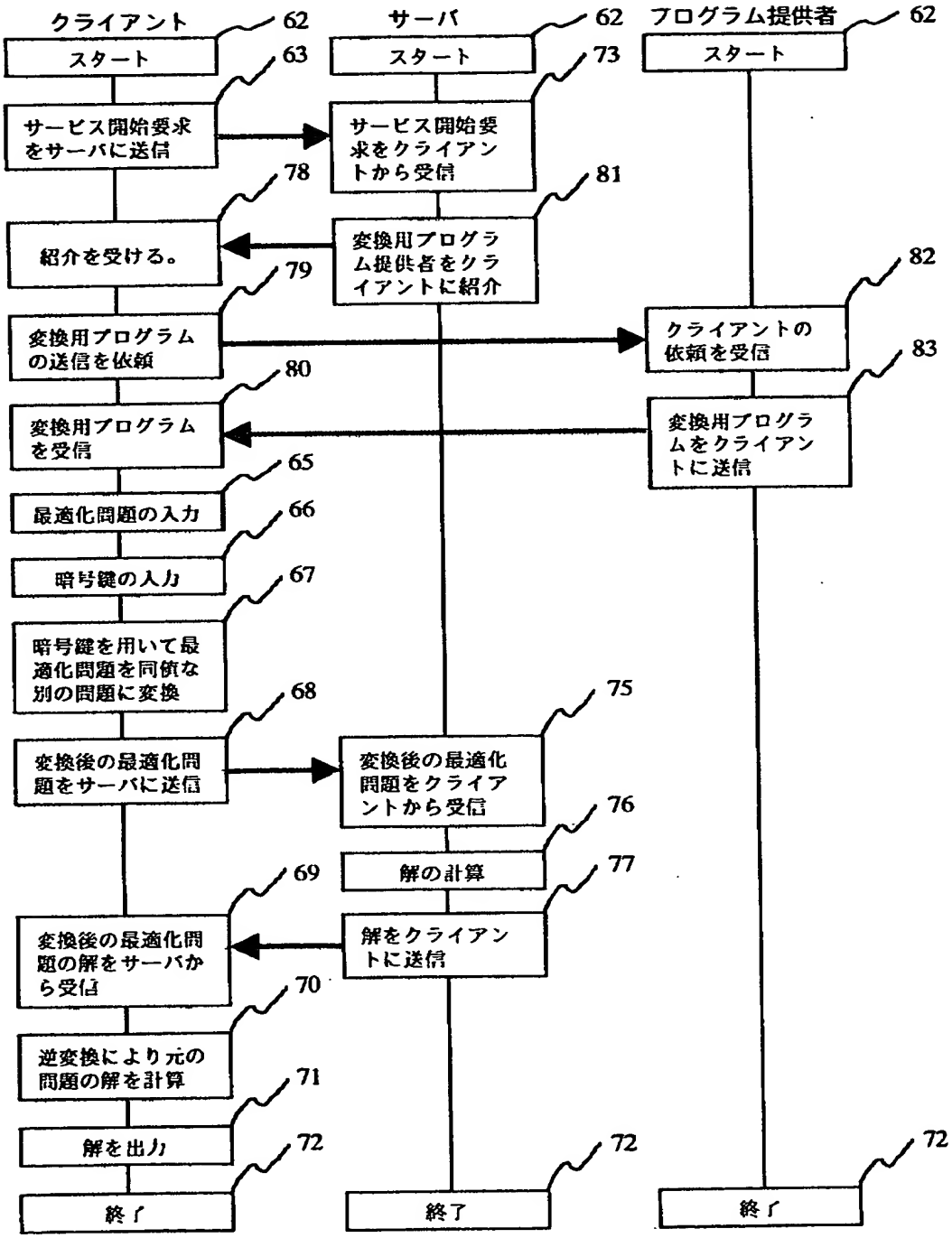
【図１２】

図12


クライアント
サーバ
62
スタート
62
スタート
63
サービス開始要求をサーバに送信
73
サービス開始要求をクライアントから受信
64
変換用プログラムをサーバから受信
74
変換用プログラムをクライアントに送信
65
最適化問題の入力
66
暗号鍵の入力
67
暗号鍵を用いて最適化問題を同値な別の問題に変換
68
変換後の最適化問題をサーバに送信
75
変換後の最適化問題をクライアントから受信
76
解の計算
69
変換後の最適化問題の解をサーバから受信
77
解をクライアントに送信
70
逆変換により元の問題の解を計算
71
解を出力
72
終了
72
終了

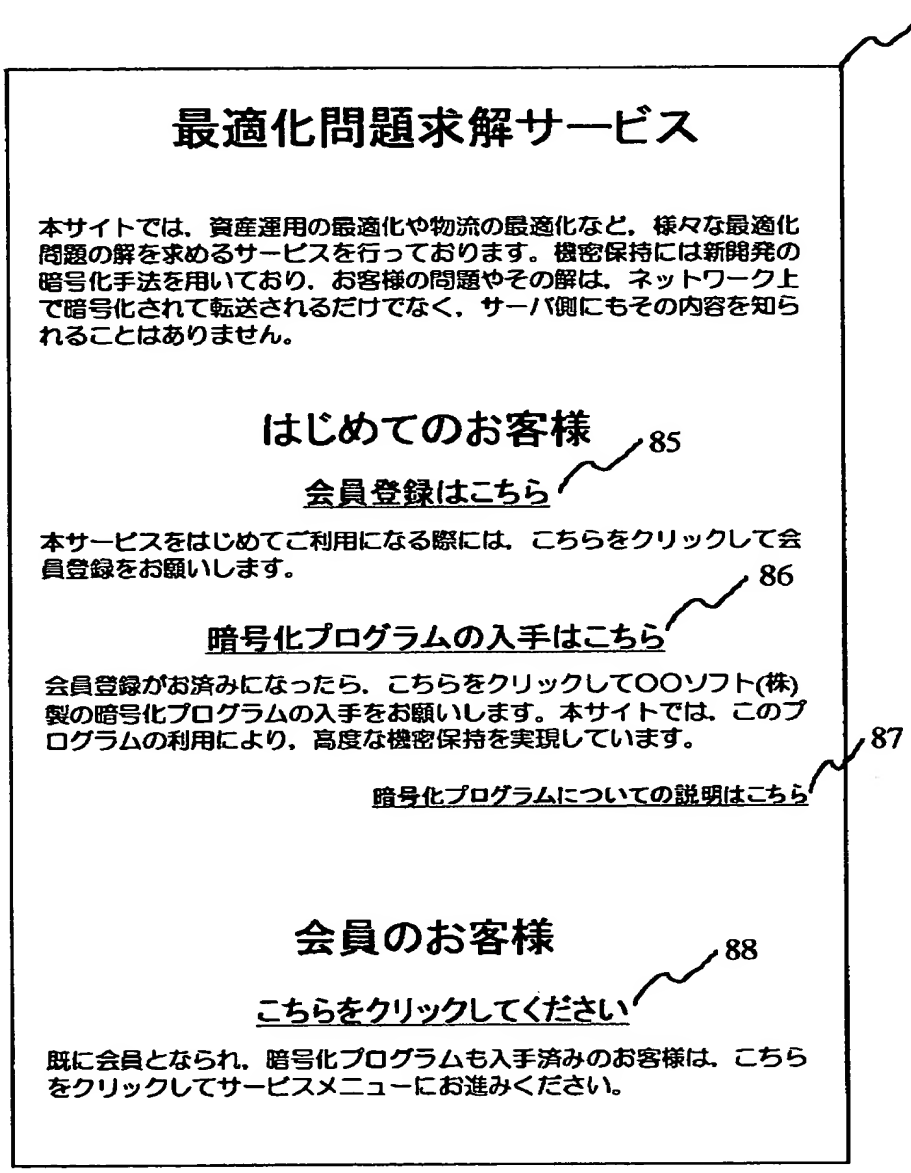
【図１３】

図13


クライアント
62
スタート
63
サービス開始要求をサーバに送信
78
紹介を受ける。
79
変換用プログラムの送信を依頼
80
変換用プログラムを受信
65
最適化問題の入力
66
暗号鍵の入力
67
暗号鍵を用いて最適化問題を同値な別の問題に変換
68
変換後の最適化問題をサーバに送信
69
変換後の最適化問題の解をサーバから受信
70
逆変換により元の問題の解を計算
71
解を出力
72
終了
サーバ
62
スタート
73
サービス開始要求をクライアントから受信
81
変換用プログラム提供者をクライアントに紹介
75
変換後の最適化問題をクライアントから受信
76
解の計算
77
解をクライアントに送信
72
終了
プログラム提供者
62
スタート
82
クライアントの依頼を受信
83
変換用プログラムをクライアントに送信
72
終了

【図１４】

図14


84
最適化問題求解サービス
本サイトでは，資産運用の最適化や物流の最適化など，様々な最適化問題の解を求めるサービスを行っております。機密保持には新開発の暗号化手法を用いており，お客様の問題やその解は，ネットワーク上で暗号化されて転送されるだけでなく，サーバ側にもその内容を知られることはありません。
はじめてのお客様
85
会員登録はこちら
本サービスをはじめてご利用になる際には，こちらをクリックして会員登録をお願いします。
86
暗号化プログラムの入手はこちら
会員登録がお済みになったら，こちらをクリックして○○ソフト(株)製の暗号化プログラムの入手をお願いします。本サイトでは，このプログラムの利用により，高度な機密保持を実現しています。
87
暗号化プログラムについての説明はこちら
会員のお客様
88
こちらをクリックしてください
既に会員となられ，暗号化プログラムも入手済みのお客様は，こちらをクリックしてサービスメニューにお進みください。

【書類名】　　要約書

【要約】

【課題】　求解システムへの最適化問題の求解依頼において、求解システム側に問題と解の情報を渡さず、かつ暗号鍵を送ることも不要とすることにある。

【解決手段】　クライアント13では、入力装置14から問題入力部16で問題を、暗号入力部17で暗号鍵10を入力し、変換行列生成部18で暗号鍵10を用いて正則行列Pと置換行列Qを生成し、問題変換部19で問題を行列P，Qを用いて暗号化して問題出力部20に出力し、問題出力部20は暗号化した問題をネットワーク8を介してサーバ24に送る。サーバ24では、問題入力部25で暗号化した問題を受け、求解部26で解を求め、解出力部27に出力し、解出力部27はネットワーク8を介して解をクライアント13に送る。クライアント13では、解入力部21で解を受け、逆変換部22で行列P，Qを用いて復号化して解出力部23に出力し、解出力部23は出力装置15に解を出力する。

【選択図】　　図６

出証特２００１－３０６５３７４

出　願　人　履　歴　情　報

識別番号　　〔０００００５１０８〕

１．変更年月日　　１９９０年　８月３１日
［変更理由］　新規登録
住　所　　東京都千代田区神田駿河台４丁目６番地
氏　名　　株式会社日立製作所